Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

National Institute of Standards and Technology
Communications Security Establishment

Initial Release: March 28, 2003

Last Update: April 04, 2003

Table of Contents

- New Guidance and Modified Guidance (Issued within the last 45 days)

New Guidance

- None

Modified Guidance

- 04/04/03: G.5 Maintaining validation compliance of software cryptographic modules
  - Changed C2 reference to CC EAL2 reference.
- 04/04/03: G.8 Revalidation Requirements
  - Added link to the revalidation regression test suit.

Overview

This Implementation Guidance document is issued and maintained by the U.S. Government's National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada, which serve as the validation authorities of the Cryptographic Module Validation Program (CMVP) for their respective governments. The CMVP is a program under which National Voluntary Laboratory Accreditation Program (NVLAP) accredited Cryptographic Module Testing (CMT) laboratories test cryptographic modules for conformance to Federal Information Processing Standard Publication (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. In addition, this program covers the testing of FIPS Approved cryptographic algorithms, including the Advanced Encryption Standard, Data Encryption Algorithm, Digital Signature Algorithm, Secure Hash Algorithm, and Skipjack Algorithm.

This document is intended to provide clarifications of the CMVP, and in particular, clarifications and guidance pertaining to the *Derived Test Requirements for FIPS PUB 140-2* (DTR), which is used by CMT laboratories to test for a cryptographic module's conformance to FIPS 140-2. Guidance presented in this document is based on responses issued by NIST and CSE to questions posed by the CMT labs, vendors, and other interested parties. *However, information in this document is subject to change by NIST and CSE.*

Each section of this document corresponds with a requirements section of FIPS 140-2, with an additional first section containing general guidance that is not applicable to any particular requirements section. Within each section, the guidance is listed according to a subject phrase. For those subjects that may be applicable to multiple requirements areas, they are listed in the area that seems most appropriate. Under each subject there is a list, including the date of issue for that guidance, along relevant assertions, test requirements, and vendor requirements from the DTR. *(Note: For each subject, there may be additional test and vendor requirements which apply.)* Next, there is section containing a question or statement of a problem, along with a resolution and any additional comments with related information. This is the implementation guidance for the listed subject.

Below is a list of where the reader can find cryptographic modules validated to 140-1 and 140-2:

- Cryptographic Module Validation List

General Issues

G.1 Implementation guidance requests to NIST and CSE

Applicable Levels:	*ALL*
Effective Dates:	*2/25/97-*
Last Modified:	*1/26/01*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

To whom should implementation guidance requests be directed? Is there a defined format for those requests?

Resolution

- *Programmatic Questions:* Questions concerning the general operation of the CMV Program can be directed to either NIST or CSE. Here are the appropriate points of contact:
  - **NIST**

    Annabelle Lee
    (301) 975-2941

    Randall J. Easter
    (301) 975-4641

    Ron Tencati
    (301) 975-3603
  - **CSE**
    Jean Campbell
    (613) 991-8121

- *Test-specific Questions:* If a vendor is under contract with a CMT lab for 140-2 or algorithm testing, then the vendor should contact the lab with any questions concerning the test requirements. This allows the lab representatives to use their expertise in FIPS 140-2 testing to answer those questions, and it acts as a filter for NIST and CSE.

  Agencies, departments, vendors not under contract with a CMT lab, and CMT labs themselves who have specific questions about a FIPS 140-2 test requirement should contact the appropriate NIST and CSE points of contact:
  - **NIST**

    Annabelle Lee
    (301) 975-2941

Randall J. Easter
(301) 975-4641

Ron Tencati
(301) 975-3603

- **CSE**
  Jean Campbell
  (613) 991-8121

All test-specific questions asking for implementation guidance shall have the following form, in order for NIST and CSE to understand the question as clearly as possible, and to provide an appropriate response:

1. Applicable statement(s) from FIPS 140-2,
2. Applicable assertion(s) from the FIPS 140-2 DTR,
3. Applicable required test procedure(s) from the FIPS 140-2 DTR,
4. A concise statement of the problem, followed by a clear and unambiguous question regarding the problem, and
5. A statement of the resolution that is being sought.

All questions should be presented in a detailed, implementation-specific format, rather than an academic or hypothetical format. This information should also include a brief description of the implementation and the FIPS 140-2 target level. All of this will enable a more efficient and timely resolution of FIPS 140-2 related questions by NIST and CSE. When appropriate, NIST and CSE will derive general guidance from the problem and response, and add that guidance to this document. Note that general questions may still be submitted, but these questions should be identified as not being associated with a particular validation effort.

****Note that NIST and CSE will only issue official, written responses when the original request is submitted in writing (e-mail and fax are also acceptable).*

Additional Comments

G.2 Completion of a validation - information that must be provided to NIST and CSE

Applicable Levels:	*ALL*
Effective Dates:	*2/25/97-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What information should be provided to NIST and CSE upon completion of validation testing, in order for a vendor to receive a validation certificate?

Resolution

The following information shall be provided to both NIST and CSE by the testing laboratory:

1. **Letter of submission** <hard copy mandatory>
   Include soft copy for reference in submission.

2. **Signature page** <hard copy mandatory>

3. **Non-proprietary Security Policy** <PDF mandatory and not locked*>
   Reference FIPS 140-2 IG 14.1 for requirements.

4. **Summary** <PDF preferred and not locked*>
   General Information page from the NIST provided FIPS 140-2 Cryptik tool. Section summaries are mandatory (briefly describe how the requirements in each section are met).

5. **Cost Recovery** <PDF preferred and not locked*>
   Provide vendor billing information.

6. **Detailed Report with Notes** <Single PDF mandatory and not locked*>
   For FIPS 140-2 the validation report must be output from the NIST provided Cryptik tool. (Note: labs may append files to the validation report for submission to NIST/CSE. For example, some labs document the physical testing in a separate word file. This may be appended to the detailed report for submission. Only ONE document is to be delivered.)

   a. (IF APPLICABLE) A *non-proprietary* version of the laboratory's physical testing report, for cryptographic modules with physical security at *level 2 and above*.

7. **Draft Certificate** <Microsoft Word mandatory>
   Use NIST provided template.

8. In addition to items 1-3 above, the lab has the option to provide *proprietary* versions of those items, but this is not required by NIST and CSE.

****NOTE: NIST and CSE must have items 2 and 5 above before a validation certificate will be issued. ****

Additional Comments

Reception of the electronic copies will determine position in the CMVP validation review queue, not when the hard copy mail shows up.

An Initial Review will be performed when the electronic copies are received by the CMVP. Following is a brief list of the initial items that are checked for consistency when a validation report package is received.

1. Are all six documents present? **Letter of submission (softcopy), Non-proprietary Security Policy, Summary, Cost Recovery Billing Information (if applicable), Detailed Report with Notes, and Draft Certificate.**

   (If a validation report package does not contain all six documents, the package will not be added to the queue. The lab will be notified.)

2. Are the name(s), version number(s), and embodiment(s) of the crypto module the same? Is the vendor name the same? **These are checked on all deliverables.**

3. Are the security levels in all documents the same? This applies to overall level and individual levels. **The security policy, summary, detailed report, and certificate are checked.**

4. Are the lists of FIPS-approved/NIST recommended and non-FIPS approved algorithms the same? **The security policy, summary, detailed report, and certificate are checked.**

   (Note: The Approved and non-Approved algorithms should be listed in AS.01.12 in the validation report.)

5. Are the certificate numbers for the FIPS-approved/NIST recommended algorithms included and are they the same? Are all the included FIPS-approved/NIST recommended algorithm modes, e.g., CBC, ECB, listed on the algorithm cert? **This information is mandatory for the detailed report with notes.**

6. For a software module, are the hardware test platform and OS listed? **This information should be included on the certificate and in the detailed report with notes.**

   The certificate must list the specific OS. Some examples are: Microsoft Windows 2000 Server, Sun Solaris 9.9, JVM v9.9.9, JRE v9.9.9.

   The validation report must list the specific OS and the hardware platform used to test the software crypto module.

7. Are there any markings in the security policy that limit copying the document (i.e. the security policy must not be proprietary)? **This is applicable to the non-propriety security policy.**

   If the security policy is marked as proprietary or copyright with no statement allowing making copies, the validation report package will be returned to the lab.

If a validation report package has a few inconsistencies, the NIST and CSE reviewers will discuss the discrepancies with the lab. If a validation report package has significant errors in these items, the validation report package will be returned to the lab. NIST OR CSE will perform this initial review, and the notification will state which organization performed this review.

Errors discovered in these items may impact other sections of the report submission. For example, if an algorithm is listed on both the FIPS and non-FIPS line – the validators do not know whether the key management and self-test requirements are applicable.

If, at any time, NIST/CSE find a fatal error in a validation report, the lab will be notified and the validation report package will either be returned to the lab or placed in hold status.

G.3 Partial validations

Applicable Levels:	*ALL*
Effective Dates:	*2/25/97-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the position of NIST and CSE regarding partial validations?

Resolution

NIST and CSE will not issue a validation certificate unless a cryptographic module meets at least Level 1 security requirements for each area in section 4 of FIPS 140-2. Note that in some cases, a requirements area might not be applicable to the cryptographic module being tested (e.g., "Mitigation of Other Attacks"). In those cases, the validation certificate will indicate "N/A" for that requirement.

Additional Comments

G.4 Design and testing of cryptographic modules

Applicable Levels:	*ALL*
Effective Dates:	*11/12/97-*
Last Modified:	*4/28/00*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What activities may CMT laboratories perform, regarding the design and testing of cryptographic modules?

Resolution

The following information is supplemental to the guidance provided by NVLAP, and further defines the separation of the design, consulting, and testing roles of the laboratories. CMV Program policy in this area is as follows:

1. A CMT Laboratory *may not* perform validation testing on a module for which the laboratory has:
    a. designed any part of the module,
    b. developed original documentation for any part of the module,
    c. built, coded or implemented any part of the module, or
    d. any ownership or vested interest in the module.
2. Provided that a CMT Laboratory has met the above requirements, the laboratory *may* perform validation testing on modules produced by a company when:
    a. the laboratory has no ownership in the company,
    b. the laboratory has a completely separate management from the company, and
    c. business between the CMT Laboratory and the company is performed under contractual agreements, as done with other clients.
3. A CMT Laboratory may perform consulting services to provide clarification of 140-2, the Derived Test Requirements, and other associated documents at any time during the life cycle of the module.

Additional Comments

Item 3 in the Resolution references "other associated documents". Included in this reference are:

- Documents developed by the CMVP staff for the Cryptographic Module testing program (e.g., Implementation Guidance, CMVP Policy, Handbook 150-17, *Cryptographic Module Testing*); and
- Implementation Guidance and Policy associated with 140-2, *Security Requirements for Cryptographic Modules*.

Also see IG G.9, regarding FSM and Security Policy consolidation and formatting.

G.5 Maintaining validation compliance of software cryptographic modules

Applicable Levels:	*ALL*
Effective Dates:	*11/12/97-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

For a validated software cryptographic module, how may such a module be implemented so that compliance with the validation is maintained?

Resolution

1. The tested/validated configuration is stated on the validation certificate. The certificate serves as the benchmark for the module-compliant configuration.
2. For level 1 Operating System Security, the software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that:
    a. the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and
    b. the software of the cryptographic module does not require modification when ported (platform specific configuration modifications are excluded).
3. For level 2 Operating System Security the software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any GPC provided that:
    a. the GPC incorporates the specified CC evaluated EAL2 (or equivalent) operating system/mode/operational settings or another compatible CC evaluated EAL2 (or equivalent) operating system with like mode and operational settings, and
    b. the software of the cryptographic module does not require modification when ported (platform-specific configuration settings are excluded).

This policy only addresses a module's operating system configuration and does not affect requirements of the other sections of FIPS 140-2. A module must meet all requirements of the level stated. The GPC used with the cryptographic software must meet all physical requirements met by the test platform listed on the validation certificate.

Additional Comments

*Note that this guidance is particularly relevant to **USERS** who are implementing a software module.*

G.6 Modules with both a FIPS mode and a non-FIPS mode

(i.e., modules containing both FIPS-approved and non-FIPS approved security methods)

Applicable Levels:	*ALL*
Effective Dates:	*3/11/98-*
Last Modified:	*4/2/98*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

How can a module be defined, when it includes both FIPS-approved and non-FIPS approved security methods?

Resolution

(4/2/98) A module that contains both FIPS-approved and non-FIPS approved security methods shall have at least one "FIPS mode of operation" - which *only* allows for the operation of FIPS-approved security methods. This means that when a module is in the "FIPS mode", a non-FIPS approved method **SHALL NOT** be used in lieu of a FIPS-approved method (For example, if a module contains both MD5 and SHA-1, then when hashing is required in the FIPS mode, SHA-1 must be used.). The operator must be made aware of which services are FIPS 140-2 compliant.

The FIPS 140-2 validation certificate will identify the cryptographic module's "FIPS mode" of operation.

The selection of "FIPS mode" does not have to be restricted to any particular operator of the module. However, each operator of the module must be able to determine whether or not the "FIPS mode" is selected.

There is no requirement that the selection of a "FIPS mode" be permanent.

Additional Comments

G.7 Relationships Among Vendors, Laboratories, and NIST/CSE

Applicable Levels:	*ALL*
Effective Dates:	*4/14/98-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the Cryptographic Module Validation Program policy regarding the relationships among vendors, testing laboratories, and NIST/CSE?

Policy

The CMT laboratories are accredited by NVLAP to perform cryptographic module validation testing to determine compliance with FIPS 140-2. NIST/CSE rely on the CMT laboratories to use their extensive validation testing experience and expertise to make sound, correct, and independent decisions based on 140-2, the Derived Test Requirements, and Implementation Guidance. Once a vendor is under contract with a laboratory, NIST/CSE will only provide official guidance and clarification for the vendor's module through the point of contact at the laboratory.

In a situation where the vendor and laboratory are at an irresolvable impasse over a testing issue, the vendor may ask for clarification/resolution directly from NIST/CSE. The vendor should use the format required by Implementation Guidance G.1 and the point of contact at the laboratory ***must*** be carbon copied. All correspondence from NIST/CSE to the vendor on the issue will be issued through the laboratory point of contact.

Additional Comments

G.8 Revalidation Requirements

Applicable Levels:	*ALL*
Effective Dates:	*8/17/2001-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the Cryptographic Module Validation Program (CMVP) policy regarding revalidation requirements and validation of a new cryptographic module that is significantly based on a previously validated module?

Policy

An updated version of a previously validated cryptographic module can be considered for a revalidation rather than a full validation depending on the extent of the modifications from the previously validated version of the module. (Note: the updated version may be, for example, a new version of an existing crypto module or a new model based on an existing model.)

There are four possible scenarios:

1. Modifications are made to hardware, software or firmware components that do not affect any FIPS 140-2 security relevant items. The CMT laboratory is responsible for identifying the necessary documentation to confirm that FIPS 140-2 security relevant items have not been affected by the modification. The vendor is then responsible to provide the applicable documentation to the CMT laboratory. Documentation may include a previous validation report, design documentation, source code, etc. The CMT laboratory will review the modifications and any associated documentation provided by the vendor and issue an explanatory letter to NIST/CSE with applicable TEs listed and

associated laboratory assessment. The assessment shall include the analysis performed by the laboratory to confirm that no security relevant TEs were affected. The updated version or release information will be posted on the FIPS 140-2 Cryptographic Module Validation List entry associated with the original cryptographic module. No new certificate will be issued.

2. Modifications are made to hardware, software or firmware components that affect some of the FIPS 140-2 security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the assertions in the FIPS 140-1 conformance test report are affected. The CMT laboratory is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient and the vendor is responsible for submitting the requested documentation to the CMT laboratory. Documentation may include a previous validation report and applicable NIST/CSE rulings, design documentation, source code, etc.

   The CMT laboratory shall identify the assertions affected by the modification and shall perform the tests associated with those assertions. This will require the CMT lab to:

   1. Review the COMPLETE list of assertion for the module embodiment and security level,
   2. Identify, from the previous validation report, the assertions that have been affected by the modification,
   3. Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
   4. Review assertions where specific Implementation Guidance (IG) was provided to confirm that the IG is still applicable.

   For example, a revision to a firmware component that added security functionality may require a change to assertions in Section 1.

   In addition to the tests performed against the affected assertions, the CMT laboratory shall also perform the regression test suite of operational tests included in **Mapping FIPS 140-2 to FIPS 140-1**. Included in the table are the ASs, TEs, VEs (AS2 for FIPS 140-2 and AS1 for FIPS 140-1, etc.), security level(s), single chip (S), multi chip embedded (ME), multi chip standalone (MS), operational test (op - x is used for the operational tests, r is used for regression test), applicable to FIPS 140-2 (M - match), and comment (describes the applicability of FIPS 140-1 results to 140-2, and may include info on the 140-2 requirement).

   The CMT laboratory shall document the test results in the associated assessments and all affected TEs shall be annotated as “re-tested.” The CMT laboratory can submit a delta conformance test report highlighting those assertions that have been modified and retested. Upon a satisfactory review by NIST/CSE, a new certificate will be issued.

3. Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module. The CMT laboratory is responsible for ensuring that the change only affects the physical enclosure (integrity) and has no operational impact on the module. The CMT laboratory must also fully test the physical security features of the new enclosure to ensure its compliance to the relevant requirements of the standard. The CMT laboratory must then submit a letter to NIST and CSE that:

   1. Describes the change (pictures may be required),
   2. State that it is a security relevant change.

3. Provide sufficient information supporting that the physical only change has no operational impact,

4. Describes the tests performed by the laboratory that confirms that the modified enclosure still provides the same physical protection attributes,

Each request will be handled on a case-by-case basis. The CMVP will accept such letters against cryptographic modules already validated to FIPS 140-1 and FIPS 140-2. Certificates will not be reissued.

An example of such a change could be a Level 2 tokens plastic encapsulation that has been reformulated or colored. Therefore the molding or cryptographic boundary has been modified. This change is security relevant as the encapsulation provides the opacity and tamper evidence requirements. But this can be handled as a letter only change with evidence that the new composition has the same physical security relevant attributes as the prior composition.

4. If modifications are made to hardware, software, or firmware components that do not meet the above criteria, then the cryptographic module will be considered a new module and must undergo a full validation testing by an accredited CMT laboratory.

If the overall Security Level of the crypto module changes or if the physical embodiment changes, e.g., from multi-chip standalone to multi-chip embedded, then the cryptographic module will be considered a new module and must undergo full validation testing by an accredited CMT laboratory.

Additional Comments

A cryptographic module that is revalidated must meet ALL current standards and IGs. The CMT laboratory is responsible for requesting from the vendor all the documentation necessary to determine whether the cryptographic module meets the current standards and IGs. This is particularly important for features/services of the cryptographic module that required a specific ruling from NIST/CSE. For example, a cryptographic module may have been validated with an implementation of Triple DES that has not been tested. If the same cryptographic module is later submitted for revalidation, this Triple DES implementation must be tested and validated against FIPS 46-3, and the cryptographic module must meet the applicable FIPS 140-2 requirements, e.g., self-tests.

G.9 FSM, Security Policy, User Guidance and Security Officer Guidance Documentation

Applicable Levels:	ALL
Effective Dates:	5/29/2002
Last Modified:	
Relevant Assertions:	
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

May a CMT lab create original documentation specified in FIPS 140-2? The specific documents in question are the FSM, Security Policy, User Guidance and Security Officer Guidance.

Policy

FSM and Security Policy:

A CMT lab may take existing vendor documentation for an existing cryptographic module (post-design and post-development) and consolidate or reformat the existing information (from multiple sources) into a set format. If this occurs, NIST and CSE shall be notified of this when the validation report is submitted. Additional details for the individual documents are provided below.

FSM: The vendor-provided documentation must readily provide a finite set of states, a finite set of inputs, a finite set of outputs, a mapping from the sets of inputs and states into the set of states (i.e., state transitions), and a mapping from the sets of inputs and states onto the set of outputs (i.e., an output function).

Security Policy: The vendor-provided documentation must readily provide a precise specification of the security rules under which a cryptographic module must operate, including the security rules derived from the requirements of FIPS 140-2 and the additional security rules imposed by the vendor.

In addition, a lab must be able to show a mapping from the consolidated or reformatted FSM and/or Security Policy back the original vendor source documentation. The mapping(s) must be maintained by the lab as part of the validation records.

Consolidating and reforming are defined as follows:

- The original source documents were prepared by the vendor (or a subcontractor to the vendor) and submitted to the laboratory with the cryptographic module.
- The laboratory extracts applicable technical statements from the original source documentation to be used in the FSM and/or Security Policy. The technical statements may **only** be reformatted to improve readability of the FSM and/or Security Policy. The content of the technical statements must not be altered.
- The laboratory may develop transitional statements in the FSM and/or Security Policy to improve readability. These transitional statements shall be specified as developed by the laboratory in the mapping.

User Guidance and Security Officer Guidance:

A CMT lab may create User Guidance, Security Officer Guidance and other non-design related documentation for an existing cryptographic module (post-design and post-development). If this occurs, NIST and CSE shall be notified of this when the validation report is submitted.

Additional Comments

Section 1 - Cryptographic Module Specification

Section 2 – Cryptographic Module Ports and Interfaces

Section 3 – Roles, Services, and Authentication

3.1 Authorized Roles

Applicable Levels:	*ALL*
Effective Dates:	*5/29/2002*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

An operator is not required to assume an authorized role to perform services where cryptographic keys and CSPs are not modified, disclosed, or substituted (e.g., show status, self-tests, or other services that do not affect the security of the module).

Resolution

Authorized roles are applicable to all callable services utilizing FIPS Approved cryptographic algorithms.

Additional Comments

Section 4 - Finite State Model

Section 5 - Physical Security

Section 6 – Operational Environment

6.1 Single Operator Mode and Concurrent Operators

Effective Dates:	3/10/2003
Last Modified:	
Relevant Assertions:	AS06.04
Relevant Test Requirements:	VE.06.04
Relevant Vendor Requirements:	TE.06.04

Background

Historically, for a FIPS 140-1 and FIPS 140-2 validated software cryptographic module on a server to meet the single user requirement of Security Level 1, the server had to be configured so that only *one* user at a time could access the server. This meant configuring the server Operating System (OS) so that only a single user at a time could execute processes (including cryptographic processes) on the server. Consequently, servers were not being used as intended.

Question/Problem

AS06.04 states: "(Level 1 Only) The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded)". What is the definition of concurrent operators in this context? Specifically, may Level 1 software modules be implemented on a server and achieve FIPS 140-2 validation? (Note: this question is also applicable to VPN, firewalls, etc.)

Resolution

Software cryptographic modules implemented in client/server architecture are intended to be used on both the client and the server. The cryptographic module will be used to provide cryptographic functions to the client and server applications. Because the module is not an application and is required to execute on an OS configured in single user mode, only *one* instance of the crypto module may be executed at any given time. When a crypto module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients. The OS enforces the requirement that only a single cryptographic process may be executed at a given time.

Additional Information

This information must be included in the non-proprietary security policy.

Section 7 – Cryptographic Key Management

Section 8 – Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Section 9 – Self-Tests

Section 10 – Design Assurance

Section 11 – Mitigation of Other Attacks

Section 12 – Appendix A: Summary of Documentation Requirements

Section 13 – Appendix B: Recommended Software Development Practices

Section 14 – Appendix C: Cryptographic Module Security Policy

14.1 Level Of Detail When Reporting Cryptographic Services

Applicable Levels:	*ALL*
Effective Dates:	*11/15/2001*
Last Modified:	
Relevant Assertions:	*AS01.02, AS01.03, AS01.12, AS01.16, AS03.14, AS10.06, AS14.02, AS14.03, AS14.04, AS14.06, AS14.07*
Relevant Test Requirements:	*TE01.03.01, TE01.03.02, TE01.16.01, TE03.14.01, TE10.06.01, TE14.07.01, TE14.07.02*
Relevant Vendor Requirements:	*VE01.03.01, VE01.03.02, VE01.16.01, VE03.14.01, VE03.14.02, VE10.06.01, VE14.07.01, VE14.07.02, VE14.07.03*

Question/Problem

What is the level of detail that the non-proprietary security policy must contain in order to describe the cryptographic service(s) implemented by a cryptographic module?

Resolution

When presenting information in the non-proprietary security policy regarding the cryptographic services that are included in the module validation, the security policy shall include, at a minimum, the following information **for each service:**

- The service name
- A concise description of the service purpose and/or use (the service name alone may, in some instances, provide this information)
- A list of Approved security functions (algorithm(s), key management technique(s) or authentication technique) used by, or implemented through, the invocation of the service.
- A list of the cryptographic keys and/or CSPs associated with the service or with the Approved security function(s) it uses.
- For each operator role authorized to use the service:
    - Information describing the individual access rights to all keys and/or CSPs
    - Information describing the method used to authenticate each role.

The presentation style of the documentation is left to the vendor. FIPS 140-2, Appendix C, contains tabular templates that provide non-exhaustive samples and illustrations as to the kind of information to be included in meeting the documentation requirements of the Standard.

Additional Comments

FIPS 140-2 requires information to be included in the module security policy which:

- Allows a user (operator) to determine when an approved mode of operation is selected (**AS01.06, AS01.16**).

- Lists all security services, operations or functions, both Approved and non-Approved, that are provided by the cryptographic module and available to operators (**AS01.12, AS03.07, AS03.14, AS14.03**).

- Provides a correspondence between the module hardware, software, and firmware components (**AS10.06**)

- Provides a specification of the security rules under which the module shall operate, including the security rules derived from the requirements of FIPS 140-2. (**AS14.02**)

- For each service, specifies a detailed specification of the service inputs, corresponding service outputs, and the authorized roles in which the service can be performed. **(AS03.14, AS14.03)**

See also to the definitions of ***Approved mode of operation*** and ***Approved security function*** in FIPS 140-2.

14.2 Level Of Detail When Reporting Mitigation Of Attacks

Applicable Levels:	*ALL*
Effective Dates:	*11/15/2001*
Last Modified:	
Relevant Assertions:	*AS 14.09*
Relevant Test Requirements:	*TE14.09.01*
Relevant Vendor Requirements:	*VE14.09.01*

Question/Problem

What is the level of detail that the non-proprietary security policy must contain that describes the security mechanism(s) implemented by the cryptographic module to mitigate other attacks?

Resolution

The level of detail describing the security mechanism(s) implemented by the cryptographic module to mitigate other attacks required to be contained in the security policy must be similar to what is found on advertisement documentation (product glossies).

Additional Information

Expired Implementation Guidance

End of Document